Dr. Steven J. Hutchison

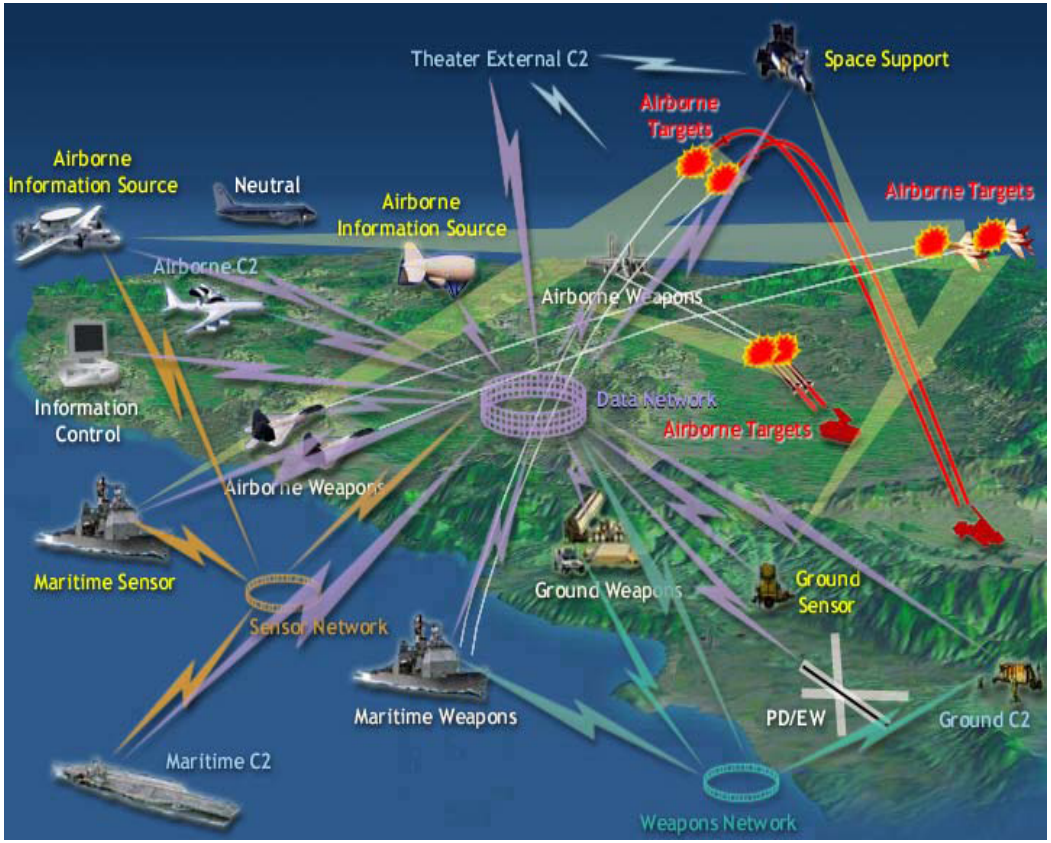
Acting DASD(DT&E)/D,TRMC

March, 2013

DISTRIBUTION STATEMENT A – Cleared for Open Publication
by OSR on January 17th, 2013 – SR case number 13-S-0851

DT&E for Complex Systems

Performance | **Reliability** | **Interoperability** | **Cybersecurity**

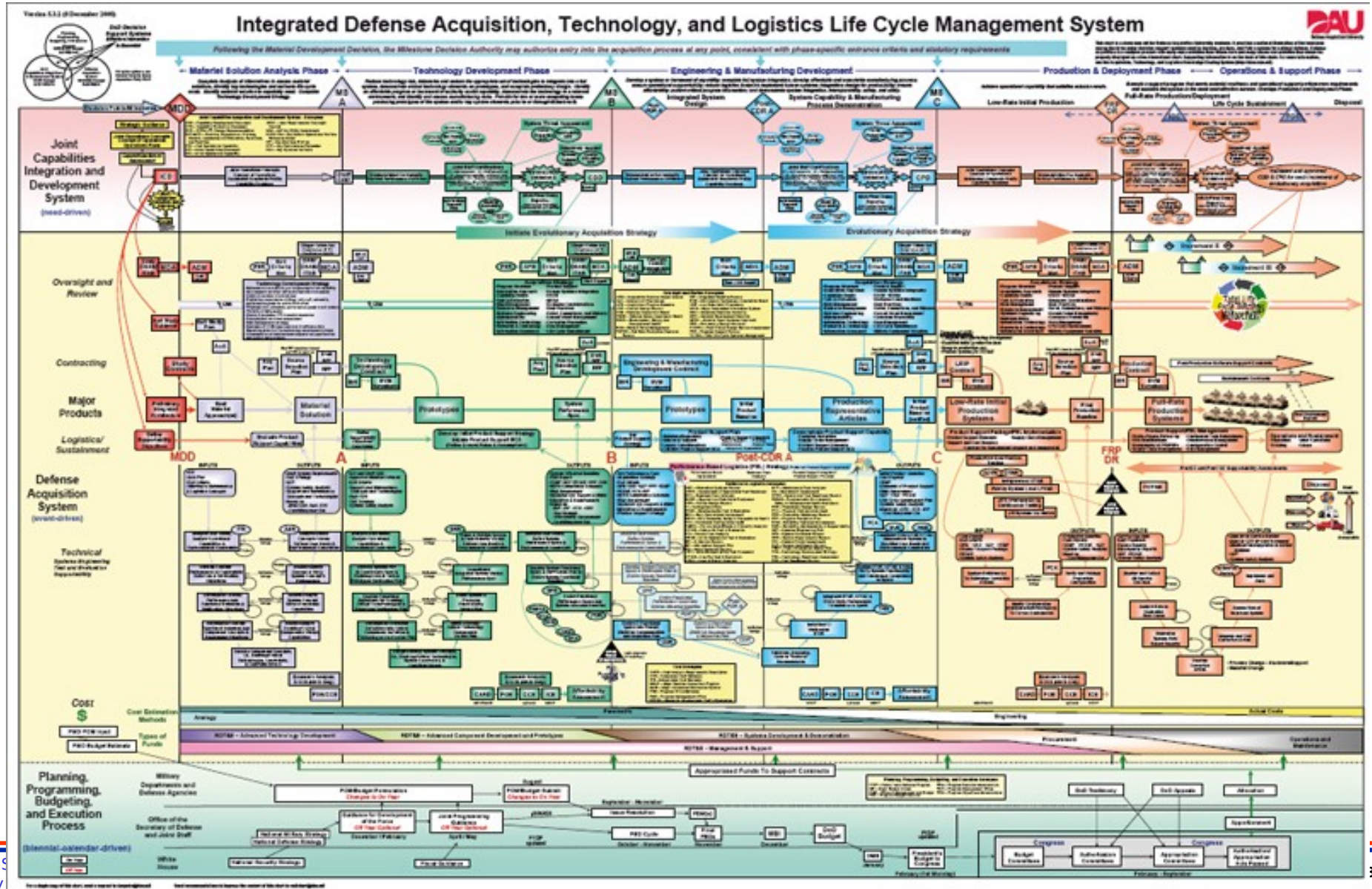


- Operations
- Test & Evaluation
- Training
- Experimentation
- Modeling & Simulation
- **Cyber Range**
- System Integration Labs
- JMETC
- JIOR

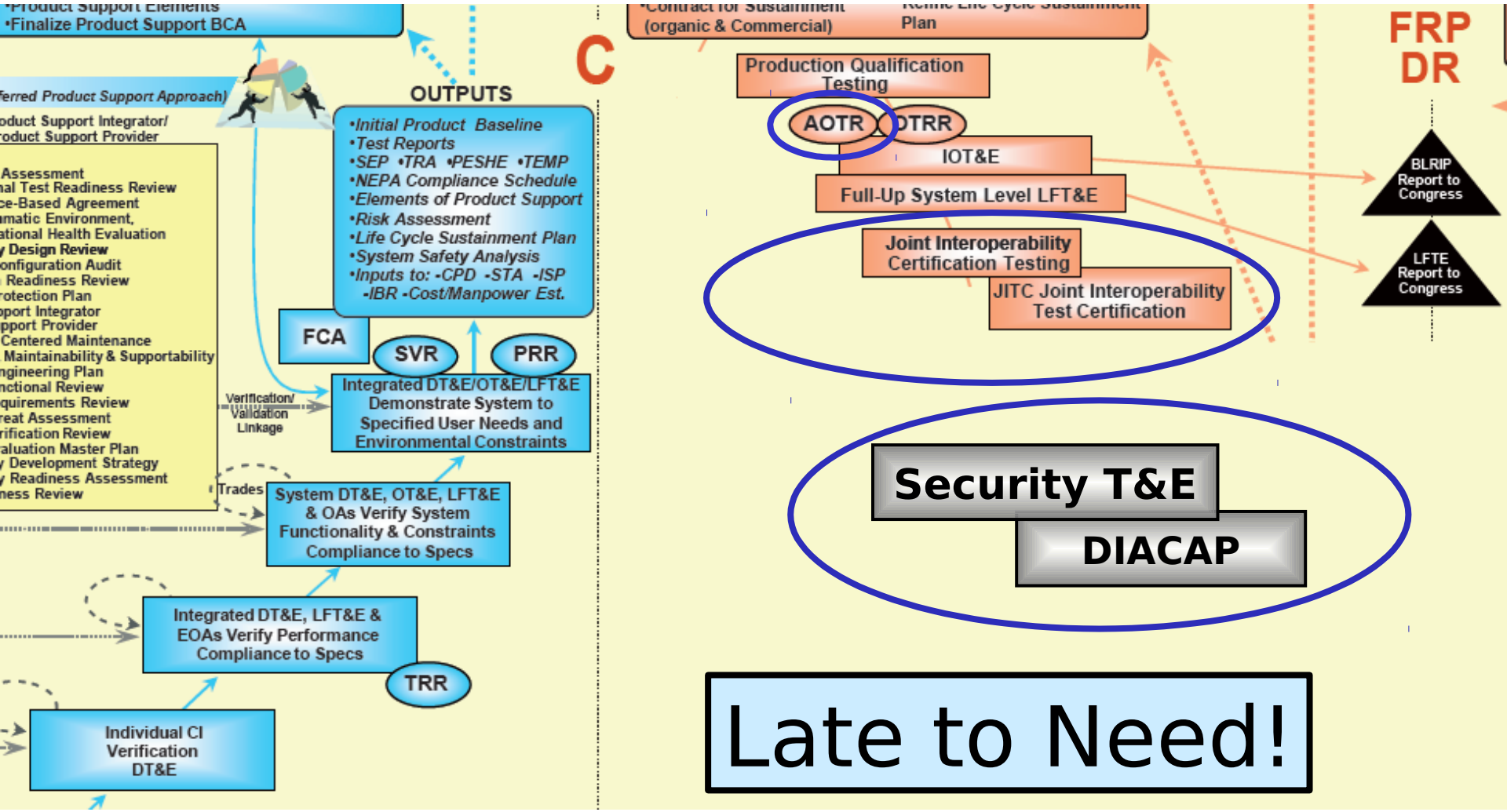
Working with stakeholders to develop a persistent, rapidly composable, secure representation of the operational environment

DISTRIBUTION STATEMENT A – Cleared for Open Publication
by OSR on January 17th, 2013 – SR case number 13-S-0851

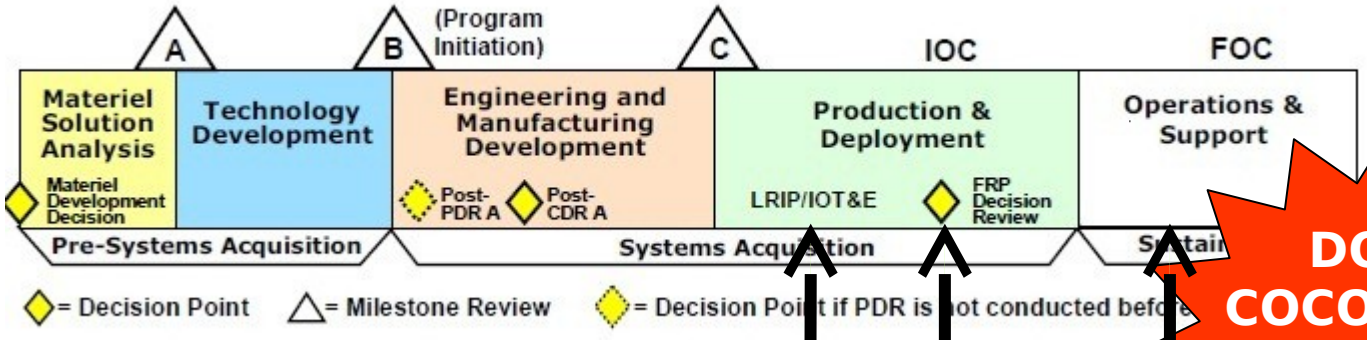
DoD Acquisition Model



Test, Evaluation, Certification



20-20 Hindsight



DOT&E COCOM/Service Interop & IA Assessments

What did we test?

What did we know?

Fielded systems:

- Interoperability issues
- IA vulnerabilities

Compliance with IA Controls and Interoperability Standards and Profiles: *necessary but not sufficient*

To reduce discovery late in the acquisition lifecycle,

- **test in mission context,**
- **against realistic threat,**

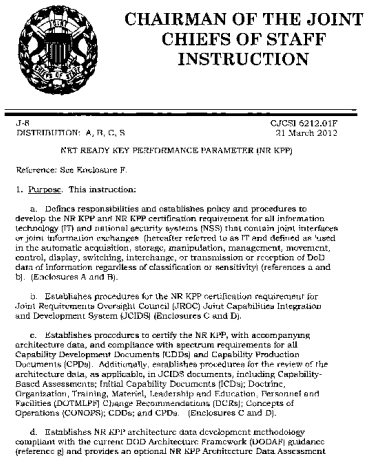
and…..

Shift Left!

in an environment suited for that purpose

Interoperability
New CJCSI 6212 Language

- **DOD Components will:**
  - Ensure the Component Developmental Test and Evaluation (DT&E), Operational Test and Ev (OT&E) processes include mission-orie assessments
- **DISA will**
  - ensure JITC leverages previous, planned and execu DT&E and OT&E tests and results to su interoperability test certification and eliminate test duplication.
  - DASD(DT&E) shall approve Developmental Test and Evaluation plans in support of Joint Interoperability Test Certification as documented in the TEMP.
  - JITC shall advise DASD (DT&E) regarding the adequacy of test planning in support of Joint Interoperability Test Certification.



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-8 CJCSI 6212.01F
DISTRIBUTION: A, B, C, S 21 March 2012

NET READY KEY PERFORMANCE PARAMETER (NR KPP)

Reference: See Enclosure F.

1. Purpose. This instruction:

a. Defines responsibilities and establishes policy and procedures to develop the NR KPP and NR KPP certification requirement for all information technology (IT) and national security systems (NSS) that contain joint interfaces or joint information exchanges (hereafter referred to as IT and defined as "used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, or transmission or reception of DoD data of information regardless of classification or sensitivity) (references a and b). (Enclosures A and B).

b. Establishes procedures for the NR KPP certification requirement for Joint Requirements Oversight Council (JROC) Joint Capabilities Integration and Development System (JCIDS) (Enclosures C and D).

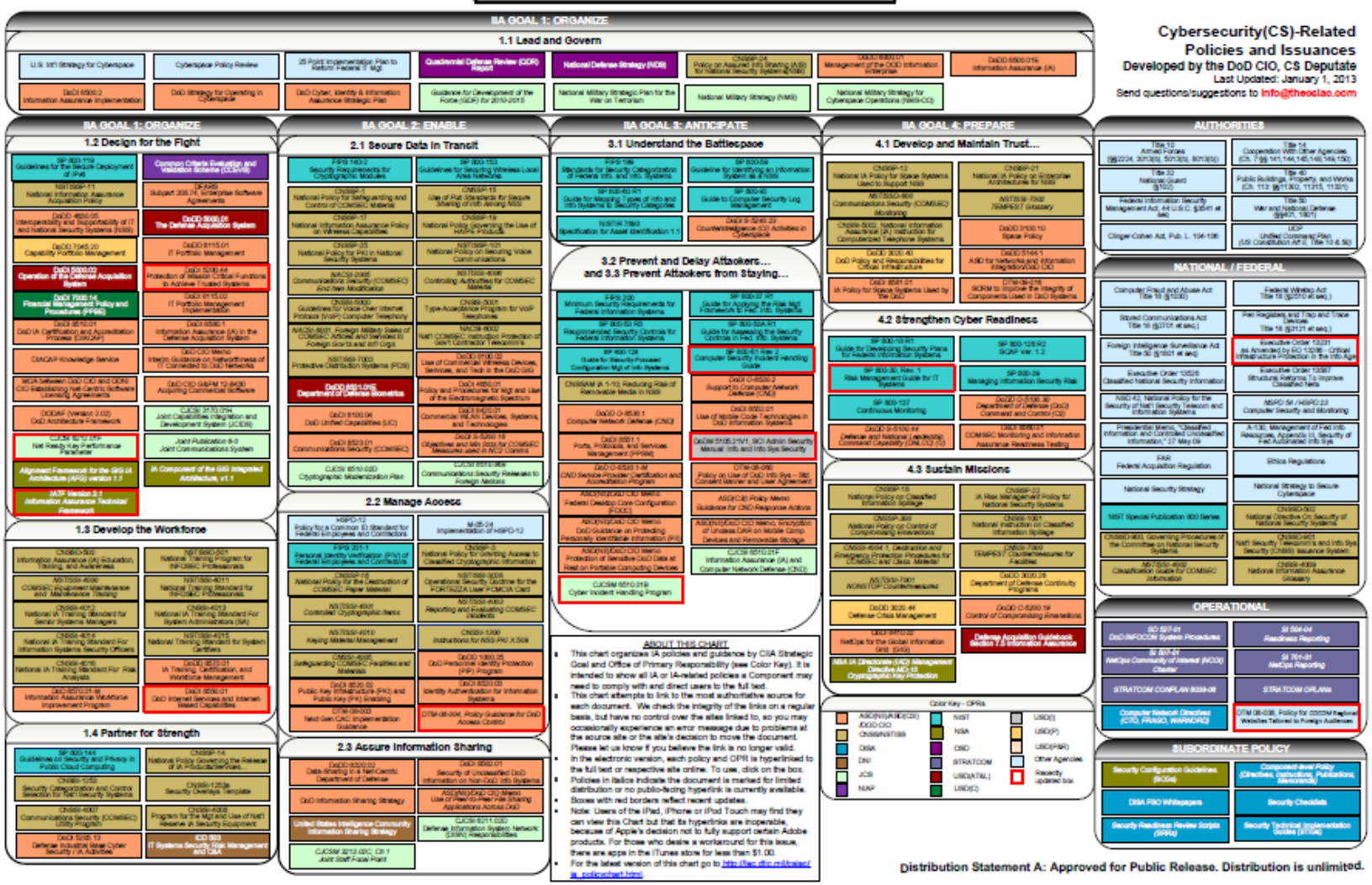
c. Establishes procedures to certify the NR KPP, with accompanying architecture data, and compliance with spectrum requirements for all Capability Development Documents (CDDs) and Capability Production Documents (CPDs). Additionally, establishes procedures for the review of the architecture data, as applicable, in JCIDS documents, including Capability-Based Assessments; Initial Capability Documents (ICDs); Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) Change Recommendations (DCRs); Concepts of Operations (CONOPS); CDDs; and CPDs. (Enclosures C and D).

d. Establishes NR KPP architecture data development methodology compliant with the current DOD Architecture Framework (DODAF) guidance (reference g) and provides an optional NR KPP Architecture Data Assessment

Increase emphasis on interoperability testing during DT&E and visibility at Defense Acquisition Boards

DISTRIBUTION STATEMENT A – Cleared for Open Publication
by OSR on January 17th, 2013 – SR case number 13-S-0851

Information Assurance Policy


Build and Operate a Trusted GIG
IIA GOAL 1: ORGANIZE
1.1 Lead and Govern
U.S. Int'l Strategy for Cyberspace
Cyberspace Policy Review
25 Point Implementation Plan to Reform Federal IT Mgt
Quadrennial Defense Review (QDR) Report
National Defense Strategy (NDS)
DoDD 8500.01E Information Assurance (IA)
DoDI 8500.2 Information Assurance Implementation
DoD Strategy for Operating in Cyberspace
DoD Cyber Identity & Information Assurance Strategic Plan
Guidance for Development of the Force (GDF) for 2010-2015
National Military Strategic Plan for the War on Terrorism
National Military Strategy (NMS)
National Military Strategy for Cyberspace Operations (NMS-CO)
IIA GOAL 1: ORGANIZE
1.2 Design for the Fight
SP 800-159 Guidelines for the Secure Deployment of IPv6
Common Criteria Evaluation and Validation Scheme (CCEVS)
NSTISSP-11 National Information Assurance Acquisition Policy
DFARS Support 2008 NL enterprise Software Agreements
DoDD 4630.05 Interoperability and Supportability of IT and National Security Systems (NSS)
DoDD 8115.01 IT Portfolio Management
DoDD 7045.20 Capability Portfolio Management
DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems
DoDD 5000.01 Operation of the Defense Acquisition System
DoDI 8115.02 IT Portfolio Management Implementation
DoDI 5000.02 Financial Management Policy and Procedures (FPPS)
DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System
DoDI 8510.01 DoD IA Certification and Accreditation Process (DIACAP)
DoD CIO Memo Interim Guidance on Netwrk'thness of IT Connected to DoD Networks
DIACAP Knowledge Service
DoD-CIO G&PM 12-8430 Acquiring Commercial Software
MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements
DoDAF (Version 2.02) DoD Architecture Framework
DoD Architecture Framework
CJCSM 3170.01H Joint Capabilities Integration and Development System (JCIDS)
CJCSM 6212.01F Net Ready Key Performance Parameter
Joint Publication 6-0 Joint Communications System
Aligned Framework for the GIG IA Architecture (AFG) version 1.1
IA Component of the GIG Integrated Architecture, v1.1
IAITF Version 2.1 Information Assurance Technical Framework
1.3 Develop the Workforce
CNSSD-500 Information Assurance (IA) Education, Training, and Awareness
NSTISSI-4011 National Training Standard for INFOSEC Professionals
NSTISSI-4009 COMSEC equipment Maintenance and Maintenance Training
NSTISSI-4011 National Training Standard for INFOSEC Professionals
CNSSI-4012 National IA Training Standard for Senior Systems Managers
CNSSI-4013 National IA Training Standard For System Administrators (SA)
CNSSI-4014 National IA Training Standard For Information Systems Security Officers
NSTISSI-4015 National Training Standard for System Certifiers
CNSSI-4016 National IA Training Standard For Risk Analysts
DoDD 8570.01 IA Training, Certification, and Workforce Management
DoDD 8570.01-M Information Assurance Workforce Improvement Program
DoDI 8500.01 DoD Internet Services and Internet Based Capabilities
1.4 Partner for Strength
SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
CNSSI-14 National Policy Governing the Release of IA Products/Services
CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
CNSSI-1253a Security Overlays Template
CNSSI-4007 Communications Security (COMSEC) Utility Program
CNSSI-4009 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment
DoDI 5205.13 Defense Industrial Base Cyber Security / IA Activities
ICD 503 IT Systems Security Risk Management and C&A
IIA GOAL 2: ENABLE
2.1 Seoure Data in Transit
FIPS 140-2 Security Requirements for Cryptographic Modules
SP 800-153 Guidelines for Securing Wireless Local Area Networks
CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
CNSSP-15 Use of Pub Standards for Secure Sharing of Info Among NSS
CNSSP-17 National Information Assurance Policy on Wireless Capabilities
CNSSP-19 National Policy Governing the Use of HAIPE Products
CNSSP-25 National Policy for PKI in National Security Systems
NSTISSP-707 National Policy on Securing Voice Communications
NACSI-2005 Communications Security (COMSEC) and Ten Modification
NSTISSI-4009 Controlling Authorities for COMSEC Materials
CNSSI-5000 Guidelines for Voice Over Internet Protocol (VoIP) Computer Telephony
CNSSI-5001 Type-Acceptance Program for VoIP Telephones
NACSI-5001 Foreign Military Sales of COMSEC Articles and Services to Foreign Gov'ts and Int'l Orgs
NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm's
NSTISSI-7003 Protective Distribution Systems (PDS)
DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG
DoD MSI-LOVE Department of Defense Biometrics
DoDI 4650.01 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum
DoDI 8100.04 DoD Unified Capabilities (UC)
DoDI 8420.01 Commercial WLAN Devices, Systems, and Technologies
DoDI 8523.01 Communications Security (COMSEC)
DoDI S-5200.16 Objectives for Min Info Sec for COMSEC Measures used in NCO Comms
CJCSI 6510.02D Cryptographic Modernization Plan
CJCSI 6511.01B Communications Security Released to Foreign Nations
2.2 Manage Access
HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors
M-05-24 Implementation of HSPD-12
FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors
CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
NSTISSP-9 National Policy for the Destruction of COMSEC Paper Material
NSTISSP-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
NTISSI-4001 Controlled Cryptographic Items
NTISSI-4002 Reporting and Evaluating COMSEC Incidents
NSTISSI-4010 Keying Material Management
CNSSI-1300 Instructions for NSS PKI X.509
NSTISSI-4005 Safeguarding COMSEC Facilities and Materials
DoDD 1300.26 DoD Personnel Exchange Program (PEP) Program
DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
DoDI 8520.03 Identity Authentication for Information Systems
DTM-08-003 Next Gen CAC Implementation Guidance
DTM-08-004, Policy Guidance for DoD Access Control
2.3 Assure Information Sharing
DoDD 8320.02 Data-Sharing in a Net-Centric Department of Defense
DoDI 8582.01 Security of Unclassified DoD Information on Non-DoD Info Systems
DoD Information Sharing Strategy
ASD(NII/DoD CIO) Memo Use of Peer-to-Peer File Sharing Applications Across DoD
United States Intelligence Community Information Sharing Strategy
CJCSM 6211.02C, Ch 1 Joint Staff Focal Point
CJCSM 6510.01B Defense Information System Network (DISN) Responsibilities
IIA GOAL 3: ANTICIPATE
3.1 Understand the Battlespace
FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems
SP 800-59 Guideline for Identifying an Information System as a NSS
SP 800-60 Pt1 Guide for Mapping Types of Info and Info Systems to Security Categories
SP 800-60 Pt2 Guide to Computer Security Log Management
NSTIR 7298 Specification for Asset Identification 1.1
DoDI S-3240.23 Counterintelligence (CI) Activities in Cyberspace
3.2 Prevent and Delay Attackers... and 3.3 Prevent Attackers from Staying...
FIPS 200 Minimum Security Requirements for Federal Information Systems
SP 800-37 R1 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
SP 800-53 R3 Recommended Security Controls for Federal Information Systems
SP 800-53A R1 Guide for Assessing the Security Controls in Fed. Info. Systems
SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems
SP 800-61 Rev 2 Computer Security Incident Handling Guide
CNSSAM IA 1-10 Reducing Risk of Removable Media in NSS
DoDI O-8530.2 Support to Computer Network Defense (CND)
DoDD 8500.1 Computer Network Defense (CND)
DoDI 8552.01 Use of Mobile Code Technologies in DoD Information Systems
DoDI 8500.1 Ports, Protocols, and Services Management (PPSM)
DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security
DoDI O-8530.1-M CND Service Provider Certification and Accreditation Program
DTM-08-060 Policy on Use of DoD Info Sys – Std Consent Banner and User Agreement
ASD(NII/DoD CIO) Memo Federal Desktop Core Configuration (FDCC)
ASD(C3I) Policy Memo Guidance for CND Response Actions
ASD(NII/DoD CIO) Memo DoD Guidance on Protecting Personally Identifiable Information (PII)
ASD(NII/DoD CIO) Memo, Encryption of Unclass DAR on Mobile Comp. Devices and Removable Storage
ASD(NII/DoD CIO) Memo Protection of Sensitive DoD Data at Rest on Portable Computing Devices
CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)
CJCSM 6510.01B Cyber Incident Handing Program
IIA GOAL 4: PREPARE
4.1 Develop and Maintain Trust...
CNSSP-12 National IA Policy for Space Systems Used to Support NSS
CNSSP-21 National IA Policy on Enterprise Architectures for NSS
NSTISSD-600 Communications Security (COMSEC) Monitoring
NSTISSI-7002 TEMPEST Glossary
CNSSI-5002 National Information Assurance (IA) Instruction for Computerized Telephone Systems
DoDD 3100.10 Space Policy
DoDD 3020.40 DoD Policy and Responsibilities for Critical Infrastructure
DoDD 5144.1 ASD for Networks and Information Integration/DoD CIO
DoDI 8581.01 IA Policy for Space Systems Used by the DoD
DTM-08-016 SCRM to Improve the Integrity of Components Used in DoD Systems
4.2 Strengthen Cyber Readiness
SP 800-16 R1 Guide for Developing Security Plans for Federal Information Systems
SP 800-126 R2 SCAP Ver. 1.2
SP 800-30 Rev. 1 Risk Management Guide for IT Systems
SP 800-39 Managing Information Security Risk
SP 800-137 Continuous Monitoring
DoDD O-5100.30 Department of Defense (DoD) Command and Control (C2)
DoDD S-5100.44 Defense and National Leadership Command Capability (DNLCC) (U)
DoDI 8580.01 COMSEC Monitoring and Information Assurance Readiness Testing
4.3 Sustain Missions
CNSSP-18 National Policy on Classified Information Spillage
CNSSP-22 IA Risk Management Policy for National Security Systems
CNSSP-300 National Policy on Control of Compromising Emanations
CNSSI-1001 National Instruction on Classified Information Spillage
CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Classi. Material
CNSSI-7000 TEMPEST Countermeasures for Facilities
NSTISSI-7001 NONSTOP Countermeasures
DoDD 3020.26 Department of Defense Continuity Programs
DoDD 3020.44 Defense Crisis Management
DoDD O-5200.19 Control of Compromising Emanations
DoDI 8410.03 NetOps for the Global Information Grid (GIG)
Defense Acquisition Guidebook, section 7.5 Information Assurance
NSA IA Directorate C4ID Management Directive MD-70 Cryptographic Key Protection
Color Key - OPRs
ASD(NII/DoD CIO) / DoD CIO
CNSS/NSTISS
DISA
DNI
JCS
NIAP
NIST
NSA
OSD
STRATCOM
USD(AT&L)
USD(C)
USD(I)
USD(P)
USD(P&R)
Other Agencies
Recently updated box
ABOUT THIS CHART
This chart organizes IA policies and guidance by CIA Strategic Goal and Office of Primary Responsibility (see Color Key). It is intended to show all IA or IA-related policies a Component may need to comply with and direct users to the full text.
This chart attempts to link to the most authoritative source for each document. We check the integrity of the links on a regular basis, but have no control over the sites linked to, so you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
In the electronic version, each policy and OPR is hyperlinked to the full text or respective site online. To use, click on the box.
Policies in italics indicate the document is marked for limited distribution or no public-facing hyperlink is currently available.
Boxes with red borders reflect recent updates.
Note: Users of the iPad, iPhone or iPod Touch may find they can view this Chart but that its hyperlinks are inoperable because of Apple's decision not to fully support certain Adobe products. For those who desire a workaround for this issue, there are apps in the iTunes store for less than $1.00.
For the latest version of this chart go to http://iac.dtic.mil/iaac/ia_policychart.html
Cybersecurity(CS)-Related Policies and Issuances
Developed by the DoD CIO, CS Deputate
Last Updated: January 1, 2013
Send questions/suggestions to Info@theciao.com
AUTHORITIES
Title 10 Armed Forces (§§2224, 3013(b), 5013(b), 8013(b))
Title 14 Cooperation With Other Agencies (Ch. 7 §§ 141,144,145,146,149,150)
Title 32 National Guard (§ 102)
Title 40 Public Buildings, Property, and Works (Ch. 113 §§ 11302, 11315, 11331)
Federal Information Security Management Act, 44 U.S.C. §3541 et seq.
Title 50 War and National Defense (§§401, 1801)
Clinger-Cohen Act, Pub. L. 104-106
UCP Unified Command Plan (US Constitution Art II. (Title 10 & 50))
NATIONAL / FEDERAL
Computer Fraud and Abuse Act Title 18 (§1030)
Federal Wiretap Act Title 18 (§2510 et seq.)
Stored Communications Act Title 18 (§2701 et seq.)
Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
Executive Order 13231 as Amended by EO 13286 - Critical Infrastructure Protection in the Info Age
Executive Order 13526 Classified National Security Information
Executive Order 13587 Structural Reforms To Improve Classified Nets
NSD-42, National Policy for the Security of Nat'l Security Telecom and Information Systems
NSPD 54 / HSPD-23 Computer Security and Monitoring
Presidential Memo, "Classified Information and Controlled Unclassified Information," 27 May 09
A-130, Management of Fed Info Resources, Appendix III, Security of Fed Automated Info Sys
FAR Federal Acquisition Regulation
Ethics Regulations
National Security Strategy
National Strategy to Secure Cyberspace
NIST Special Publication 800 Series
National Directive On Security of National Security Systems
CNSSD-500 Information Assurance (IA) Education, Training, and Awareness
CNSSD-600, Governing Procedures of the Committee on National Security Systems
NSTISSI-4009 National Information Assurance Glossary
NSTISSI-4002 Classification Guide for COMSEC Information
OPERATIONAL
SD 527-01 DoD/INFOCON System Procedures
SI 504-04 Readiness Reporting
SI 527-02 NetOps Community of Interest (NCOI) Charter
SI 701-01 NetOps Reporting
STRATCOM CONPLAN 8039-08
STRATCOM ORLANs
Computer Network Directives (CTO, FRAGO, WARNORD)
DTM 08-038, Policy for CDCOM Regional Websites Tailored to Foreign Audiences
SUBORDINATE POLICY
Security Configuration Guidelines (SCGs)
Component-level Policy (Directives, Instructions, Publications, Memoranda)
DISA FSO Whitepapers
Security Checklists
Security Readiness Review Scripts (SRRs)
Security Technical Implementation Guides (STIGs)
Distribution Statement A: Approved for Public Release. Distribution is unlimited.

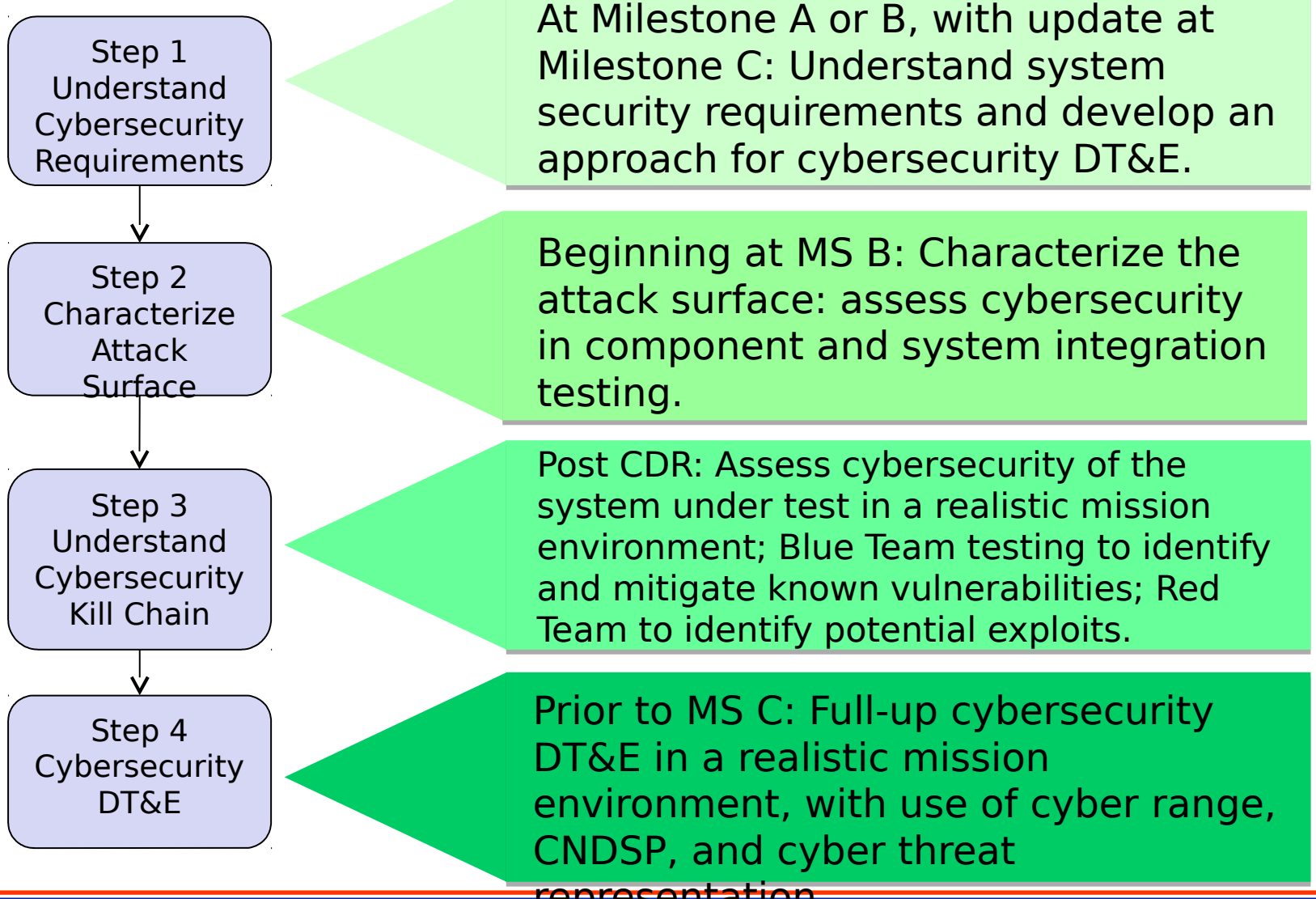
Information Assurance
Pending Revisions to DoD 8500

- **Adopt the term: “cybersecurity”**
- **Implement Risk Management Framework (RMF) instead of Mission Assurance Category/Confidentiality Level (MAC/CL)**
  - new guidance from the National Institute of Standards and Technology (NIST) and Committee on National Security Systems Instruction (CNSSI) documents on cybersecurity
- **Lexicon Changes**
  - Certification and Accreditation becomes Assessment and Authorization
  - Designated Approving Authority (DAA) becomes Authorizing Official (AO)
  - Certifying Authority becomes Security Control Assessor
  - Threat: any event with potential to cause harm to the network
  - Vulnerability: absence/weakness of safeguards to protect the network

Seeking to implement oversight of test planning in support of cybersecurity C&A(A&A)

DISTRIBUTION STATEMENT A – Cleared for Open Publication
by OSR on January 17th, 2013 – SR case number 13-S-0851

Cybersecurity DT&E Process


Step 1
Understand Cybersecurity Requirements
At Milestone A or B, with update at Milestone C: Understand system security requirements and develop an approach for cybersecurity DT&E.
Step 2
Characterize Attack Surface
Beginning at MS B: Characterize the attack surface: assess cybersecurity in component and system integration testing.
Step 3
Understand Cybersecurity Kill Chain
Post CDR: Assess cybersecurity of the system under test in a realistic mission environment; Blue Team testing to identify and mitigate known vulnerabilities; Red Team to identify potential exploits.
Step 4
Cybersecurity DT&E
Prior to MS C: Full-up cybersecurity DT&E in a realistic mission environment, with use of cyber range, CNDSP, and cyber threat representation

DISTRIBUTION STATEMENT A – Cleared for Open Publication
by OSR on January 17th, 2013 – SR case number 13-S-0851

Conclusion

- Improve production readiness
- Reduce discovery in IOT&E
- Improve acquisition outcomes

To ensure timely fielding of proven capabilities to the Warfighter …

Shift Left!

DISTRIBUTION STATEMENT A – Cleared for Open Publication
by OSR on January 17th, 2013 – SR case number 13-S-0851

Questions?

DISTRIBUTION STATEMENT A – Cleared for Open Publication
by OSR on January 17th, 2013 – SR case number 13-S-0851